Informationssikkerhedspolitik

Godkendt af byrådet den xx.xx.2022

Rebild
KOMMUNE

Indledning

Informationssikkerhedspolitikken (herefter sikkerhedspolitikken) er den overordnede beskrivelse af rammerne for beskyttelse af information i Rebild Kommune. Da kommunen behandler store mængder af informationer – herunder personoplysninger, skal brugen og håndteringen af data foregå betryggende og med et passende sikkerhedsniveau, som borgere og virksomheder har tillid til. Rebild Kommune følger principperne i den internationale standard for informationssikkerhed, ISO27001, som vedtaget i den fællesoffentlige digitaliseringsstrategi 2016-2020. Standarden skal betragtes som en referenceramme, der anvendes som rettesnor og redskab for tilrettelæggelse og styring af informationssikkerhed i kommunen.

Formål og principper

Det overordnede formål med sikkerhedspolitikken er at sikre, at anvendelsen af informationer sker efter gældende lovgivning, anerkendte standarder og udmeldinger fra Datatilsynet.[1] Enhver, der arbejder med, eller får berøring med kommunens informationer og informationssystemer, har derfor et medansvar for at opretholde den generelle informationssikkerhed.

Sikkerhedspolitikken udmøntes gennem implementering af relevante sikringsforanstaltninger, som skal beskytte information med udgangspunkt i tre centrale begreber:

- Fortrolighed – at information ikke kommer til uvedkommendes kendskab
- Integritet – at information forbliver pålidelig, korrekt og intakt
- Tilgængelighed – at relevant information kan tilgås og anvendes, når der er behov for det.

For at understøtte sikkerhedsindsatsen og fastholde informationssikkerheden, skal følgende overholdes:

- Der skal være regler og procedurer, som sikrer, at informationssikkerhed er en integreret del af driften og det daglige arbejde.
- Brugen af eksterne konsulenter, samarbejdspartnere og leverandører skal via kontrakt- og leverandørstyring sikre, at eksterne parter lever op til Rebild Kommunes niveau for informationssikkerhed.
- Der skal løbende arbejdes med evaluering og forbedringer af regler og procedurer, så informationssikkerheden tilpasses Rebild Kommunes risikovillighed, det reelle trusselsbillede, teknologi, lovgivning og best practice for området.
- Medarbejderne skal løbende uddannes i informationssikkerhed, så de har et vidensniveau, der er passende for deres arbejdsområde.

Gyldighed og omfang

Sikkerhedspolitikken omfatter enhver form for data, der ejes, opbevares eller behandles af kommunen og kommunens databehandlere. Dette gør sig gældende uanset hvilket medie, informationen er lagret på og uanset hvordan data fremstår eksempelvis elektronisk, papirbaseret, i tale, transmitteret eller filmisk form. Sikkerhedspolitikken er gældende for alle, der udfører opgaver eller hverv for kommunen, herunder:

- Ansatte, både fastansatte, midlertidigt ansatte, vikarer og lign.
- Medlemmer af byrådet

[1] Referencer:
- Databeskyttelsesforordningen (GDPR), jf. Europa-Parlamentets og Rådets Forordning af 2016/679 af 27. april 2016.
- Databeskyttelsesloven, jf. lov nr. 502 af 23. maj 2018.
- International standard for informationssikkerhed, jf. ISO/IEC 27001:2017.

- Eksterne samarbejdspartnere, eksempelvis personer og virksomheder, der udfører opgaver for kommunen

Kommunens sikkerhedspolitik gælder for alle lokaliteter, hvor der sker en anvendelse og bearbejdning af kommunens informationer fx på rådhus, institutioner, hjemmearbejdspladser eller adgang via mobil.

Organisering og ansvar

Det er en ledelsesmæssig opgave at sikre, at behandlingen af informationer sker på en sikkerhedsmæssig forsvarlig måde, og det er i overensstemmelse med sikkerhedspolitikken. Derfor er ansvaret entydigt forankret hos kommunens ledelse på lige fod med ansvaret for fx økonomi og personale. Informationssikkerhedspolitikken godkendes af Rebild Kommunes byråd.

Kommunaldirektøren er øverste sikkerhedsansvarlige og har i samarbejde med informationssikkerhedsudvalget (herefter sikkerhedsudvalget) ansvar for at udmønte og forankre politikken i organisationen.

Sikkerhedsudvalget vedligeholder sikkerhedspolitikken og -regler samt foretager risikovurderinger i samarbejde med system- og dataejere og systemforvaltere. Desuden sørger sikkerhedsudvalget for at orientere ledere og medarbejdere om informationssikkerhed, så de har den nødvendige viden til at håndtere informationer på sikker vis.

Funktionsleder for It og Digitalisering er ansvarlig for den daglige ledelse af sikkerhedsarbejdet, herunder at sikre prioritering og opfølgning på de opgaver, der er forbundet med indsatsen.

Alle ansatte er ansvarlige for at efterleve politik, sikkerhedsregler og procedurebeskrivelser samt rapportere risici og hændelser via Servicedesk.

Sikkerhedsniveau

Rebild Kommune forholder sig aktivt til trusler mod informationssikkerheden og iværksætter realistiske og tilstrækkelige handlinger for at sikre et tilstrækkeligt sikkerhedsniveau.

Sikkerhedsniveauet fastlægges som en afvejning af hensynet til både sikkerhed, brugervenlighed og omkostninger. Kommunen skal ikke sikre sig for enhver pris, men være bevidst om enhver risiko.

Sikkerhedsniveauet fastlægges på baggrund af konkrete risikovurderinger. Ledelsen deltager aktivt i risikovurderingerne og er ansvarlig for at vurdere trusler og konsekvenser.

Risikovurderingerne foretages minimum årligt samt ved større ændringer i systemanvendelsen, nye trusler eller ved leverandørskifte.

Med udgangspunkt i risikovurderingerne prioriterer ledelsen de nødvendige foranstaltninger for at sikre, at Rebild Kommune fastholder det ønskede niveau for informationssikkerhed.

Sikkerhedsbrud og overtrædelser

Alle medarbejdere skal rapportere risici og sikkerhedshændelser til nærmeste leder og Servicedesk.

Alle, der behandler data og informationer på vegne af Rebild Kommune, er forpligtet til at efterleve den til enhver tid gældende sikkerhedspolitik med tilhørende retningslinjer, forretningsgange og relaterede bilag. Enhver overtrædelse kan efter omstændighederne medføre sanktioner.

Såfremt en medarbejder er vidende om, at kommunens sikkerhedspolitik overtrædes, skal dette meddeles til ledelsen.

Udmøntning

Principperne i sikkerhedspolitikken omsættes til sikkerhedsregler, som omfatter administrative, fysiske og tekniske sikringsforanstaltninger. Reglerne godkendes af sikkerhedsudvalget. Udmøntning af reglerne sker i form af procedurer, vejledninger, aftaler med kommunens leverandører, kontrolforanstaltninger samt uddybende it-sikkerhedsregler.

Sikkerhedsreglerne kan tilgås via [link til Skoven-indsættes].

Vedligeholdelse af informationssikkerhedspolitikken

Sikkerhedspolitikken godkendes af Byrådet først i hver byrådsperiode. Sikkerhedsreglerne vurderes én gang årligt for at sikre, at den er i overensstemmelse med de aktuelle mål eller risikobillede samt gældende lovgivning, som Rebild Kommune arbejder efter. Sikkerhedsudvalget har ansvaret for at gennemføre vurderingen. Ved ændringer til sikkerhedspolitikken eller -regler, skal direktionen orienteres om resultatet af vurderingen inden offentliggørelse.

Versionshistorik

Version:

Godkendt af:

Gyldighedsdato:

Næste opdatering:

Ændringslog: